

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-067336

(43)Date of publication of application : 07.03.2003

(51)Int.Cl.

G06F 15/00

(21)Application number : 2001-255996

(71)Applicant : BANK OF TOKYO-MITSUBISHI LTD

(22)Date of filing : 27.08.2001

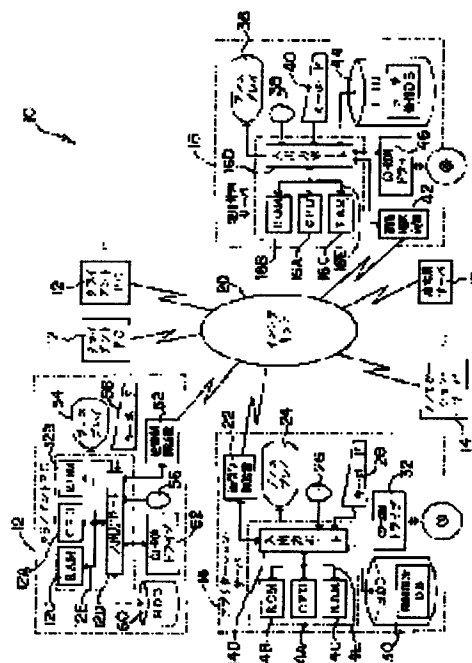
(72)Inventor : NAKAMORI YUKIO
KAMEDA HIROKI

(54) COMPUTER SYSTEM AND USER MANAGEMENT METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To control use of a system by an individual user according to use authority decided to each the individual user without impairing maintainability and security.

SOLUTION: When transmitting a user ID or the like to an operation management server 16 through a PC 12 to request login in use of an MI system 10 including a plurality of application systems realized by individual servers 14, the operation management server 16 issues a ticket after checking the user ID, and displays a menu screen capable of being used by only the application system whose use authority the user has, on a display 54. Various functions provided by the individual application system are used by transmitting the tickets to the corresponding server 14, and the server 14 authenticates the user by the ticket, and provides the requested function only when the user has the use authority of the requested function.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-67336

(P2003-67336A)

(43) 公開日 平成15年3月7日 (2003.3.7)

(51) Int.Cl.⁷

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

テーマコード(参考)

3 3 0 B 5 B 0 8 5

審査請求 有 請求項の数 9 O L (全 18 頁)

(21) 出願番号 特願2001-255996(P2001-255996)

(22) 出願日 平成13年8月27日(2001.8.27)

特許法第64条第2項ただし書の規定により図面第8図、
9図の一部は不掲載とした。

(71) 出願人 598049322

株式会社東京三菱銀行

東京都千代田区丸の内2丁目7番1号

(72) 発明者 中森 行雄

東京都目黒区青葉台4-8-6 株式会社

東京三菱銀行内

(72) 発明者 亀田 浩樹

東京都目黒区青葉台4-8-6 株式会社

東京三菱銀行内

(74) 代理人 100079049

弁理士 中島 淳 (外3名)

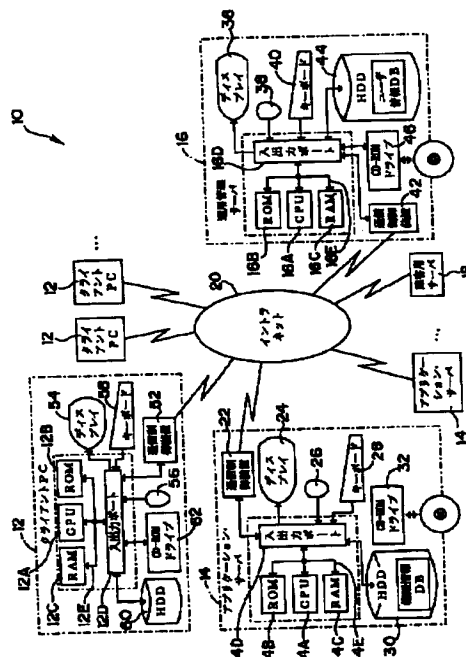
Fターム(参考) 5B085 AE02 BC01 BE07 BG07 CE01

(54) 【発明の名称】 コンピュータ・システム及びユーザ管理方法

(57) 【要約】

【課題】 個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メンテナンス性やセキュリティ性を損なうことなく実現する。

【解決手段】 個々のサーバ14によって実現される複数のアプリケーション・システムを含むM Iシステム10を利用するにあたり、P C12を介して運用管理サーバ16へユーザID等を送信してログインを要求すると、サーバ16はユーザIDのチェック後にチケットを発行し、ユーザが利用権限を有するアプリケーション・システムのみ利用可能なメニュー画面をディスプレイ54に表示させる。個々のアプリケーション・システムが提供する各種機能の利用は、対応するサーバ14へチケットを送信することで行われ、サーバ14ではチケットによるユーザ認証を行った後に、要求された機能の利用権限をユーザが有している場合にのみ要求された機能を提供する。



【特許請求の範囲】

【請求項1】 ユーザによって操作される端末と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システムであって、前記コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、前記複数種のアプリケーション・システムのうち前記個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第1権限情報を記憶する第1記憶手段と、前記複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して設けられ、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有している機能を特定するための第2権限情報を記憶する第2記憶手段と、前記コンピュータ・システムへのユーザのログイン要求に対し、前記第1記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、前記第1権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可する確認・許可手段と、を備え、

前記第2記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、対応する第2記憶手段に記憶されている第2権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供することを特徴とするコンピュータ・システム。

【請求項2】 前記確認・許可手段は、ユーザが個々のアプリケーション・システムの利用を要求するためのメニュー画面に、前記正当な利用者であることを確認できたユーザが利用権限を有しているアプリケーション・システムのみを選択肢として表示させることで、前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可することを特徴とする請求項1記載のコンピュータ・システム。

【請求項3】 前記第2記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、前記提供可能な機能の利用をユーザが要求するための画面に、前記ユーザが利用権限を有している機能のみを選択肢として表示させるか、又は、前記ユーザが利用権限を有していない機能の利用が前記ユーザから要求された場合に利用権限外であることを報知することで、前記ユーザが利用権限を有している機能のみを前記ユーザに提供する

ことを特徴とする請求項1記載のコンピュータ・システム。

【請求項4】 前記第2権限情報は、対応するアプリケーション・システムがユーザに提供可能な機能についてのユーザの利用権限のレベルを複数のクラスに分類したときに、前記アプリケーション・システムの利用権限を有する個々のユーザが前記複数のクラスの何れに属するかを表す情報、又は、対応するアプリケーション・システムがユーザに提供可能な各機能について、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有するか否かを各々表す情報であることを特徴とする請求項1記載のコンピュータ・システム。

【請求項5】 前記第2記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な複数種の機能のうちの何れかの機能の利用がユーザから要求される毎に、利用が要求されている機能の利用権限を前記ユーザが有しているか否かを判断することを特徴とする請求項1記載のコンピュータ・システム。

【請求項6】 前記確認・許可手段は、正当な利用者であることを確認できたユーザに対し、前記ユーザが利用権限を有するアプリケーション・システムを前記ユーザが利用する際に用いるためのチケット情報を与え、前記複数種のアプリケーション・システムの各々は、自システムがユーザに提供可能な機能の利用を要求しているユーザが正当なチケット情報を所持しているか否かを判断することで、前記利用を要求しているユーザが自システムの利用権限を有している正当な利用者か否かを判定することを特徴とする請求項1記載のコンピュータ・システム。

【請求項7】 前記確認・許可手段は、前記チケット情報として、所定の情報を秘密鍵によって暗号化した情報を用い、前記複数種のアプリケーション・システムの各々は、前記ユーザから前記端末を介して送信されたチケット情報を公開鍵によって復号化した際に前記所定の情報が再現されるか否かに基づいて、前記ユーザが正当なチケット情報を所持しているか否かを判断することを特徴とする請求項6記載のコンピュータ・システム。

【請求項8】 前記確認・許可手段に異常が生じた場合に、前記コンピュータ・システムへのユーザのログイン要求に対し、前記ユーザのユーザIDを付加することで前記ユーザがアプリケーション・システムを利用する際に使用可能な障害用チケット情報をユーザに与える障害チケット提供手段を更に備えたことを特徴とする請求項6記載のコンピュータ・システム。

【請求項9】 ユーザによって操作される端末と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システムに適用可能なユーザ管理方法であって、

(3)

特開2003-67336

3

前記コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、前記複数種のアプリケーション・システムのうち前記個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第1権限情報を第1記憶手段に記憶しておくと共に、

前記複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して設けられた第2記憶手段に、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有している機能を特定するための第2権限情報を記憶しておく、

前記コンピュータ・システムへのユーザのログイン要求に対し、前記第1記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、

正当な利用者であることを確認できたユーザに対し、前記第1権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可し、

前記第2記憶手段が設けられているアプリケーション・システムに対し、ユーザより前記アプリケーション・システムが提供可能な機能の利用が要求された場合に、対応する第2記憶手段に記憶されている第2権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供することを特徴とするユーザ管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンピュータ・システム及びユーザ管理方法に係り、特に、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システム、及び該コンピュータ・システムに適用可能なユーザ管理方法に関する。

【0002】

【従来の技術】コンピュータ・システムにおいて、予め登録された正当なユーザ以外の他者の不正利用を排除することは、一般に、正当なユーザのユーザ情報（例えばユーザIDとパスワード）を予め記憶しておき、コンピュータ・システムにログインしようとしているユーザに対してユーザ情報の送信を要求し、パーソナル・コンピュータ（PC）等の端末を介してユーザ側から送信されたユーザ情報を予め記憶されているユーザ情報と照合し、ログインしようとしているユーザが正当なユーザか否かを判断することによって行われる。コンピュータ・システムが提供する機能（サービス）は、正当なユーザであると判断されて正常にログインできたユーザのみが利用可能となる。

【0003】また、コンピュータ・システムが提供する

4

種々の機能の中には、正当なユーザのうちの一部のユーザに対してのみ利用を許可している機能が存在している場合もある。このような場合、コンピュータ・システムは、提供機能に対する個々のユーザの利用権限を規定する権限情報を予め記憶しておき、ログインしたユーザの権限情報を参照し、ログインした個々のユーザに対して個々のユーザが利用権限を有している機能のみを提供するように構成される。なお、権限情報はユーザ情報と共に単一のデータベース（DB）に保存されることが一般的であった。

【0004】

【発明が解決しようとする課題】ところで、金融機関では、業務の効率向上・顧客へのサービス向上を目的として、かなり以前より業務の機械化に取り組んでいるが、金融機関における業務は多種多様であるために、互いに異なる業務の遂行を支援するための互いに独立した多数種のアプリケーション・システムが存在しており、各アプリケーション・システムを利用するためには、個々のアプリケーション・システム毎に設けられた専用端末を操作して各アプリケーション・システムに個別にログインする必要があった。このため、各種のアプリケーション・システムを統合して単一のコンピュータ・システムを構築することが検討されている。

【0005】しかしながら、上記のように互いに異なるサービスを提供する複数種のアプリケーション・システムを統合して単一のコンピュータ・システムを構築した等の場合、例えば或るアプリケーション・システムの権限情報が、ユーザの利用権限のレベルを複数のクラスに分類したときに個々のユーザが何れのクラスの何れに属するかを表す情報であるのに対し、別のアプリケーション・システムの権限情報は、アプリケーション・プログラムがユーザに提供可能な全機能について個々のユーザが利用権限を有するか否かを各々規定する情報である等のように、権限情報の体系自体からして個々のアプリケーション・システム毎に相違していることが多い。

【0006】このような場合に、個々のアプリケーション・システムに対応する権限情報を統合し、ユーザ情報と共に単一のDBに保存したとすると、DBに保存する情報のデータ構造が極めて複雑になるので、例えばユーザの新規追加、或いは特定のアプリケーション・システムに対応する権限情報のデータ構造の変更（例えば利用権限のレベルを分類するクラス数の変更や、個々のユーザの利用権限を詳細に定めたテーブルの追加等）を行う必要が生じた場合の作業が非常に煩雑となり、メンテナンス性が大幅に低下するという問題がある。

【0007】また、上記のように、個々のユーザを単位としてコンピュータ・システムの利用を管理するための情報（各アプリケーション・システムに対応する権限情報やユーザ情報）をDBに一元管理すると、正当なユーザ以外の他者が、コンピュータ・システムに侵入して上

10

20

30

40

50

(4)

特開2003-67336

5

記のDBに保管されている情報を書き替えることで、コンピュータ・システムを自由に不正利用することも可能となってしまうため、セキュリティの面からも好ましくない。

【0008】本発明は上記事実を考慮して成されたもので、個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メンテナンス性やセキュリティ性を損なうことなく実現できるコンピュータ・システム及びユーザ管理方法を得ることが目的である。

【0009】

【課題を解決するための手段】上記目的を達成するために請求項1記載の発明に係るコンピュータ・システムは、ユーザによって操作される端末と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システムであって、前記コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、前記複数種のアプリケーション・システムのうち前記個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第1権限情報を記憶する第1記憶手段と、前記複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して設けられ、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有している機能を特定するための第2権限情報を記憶する第2記憶手段と、前記コンピュータ・システムへのユーザのログイン要求に対し、前記第1記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、前記第1権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可する確認・許可手段と、を備え、前記第2記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、対応する第2記憶手段に記憶されている第2権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供することを特徴としている。

【0010】請求項1記載の発明に係るコンピュータ・システムは、ユーザによって操作される端末（PC等から成るクライアント・コンピュータであってもよいし、TSS端末装置等の端末であってもよい）と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システム（コ

6

ンピュータが各アプリケーション・プログラムを実行することで実現されるシステム）を含んで構成されている。なお、前記プログラム群を実行するコンピュータは単一のコンピュータであってもよいが、複数台のコンピュータで前記プログラム群を分担して実行する構成の方が、コンピュータに加わる負荷を分散させることができるので好ましい。

【0011】請求項1記載の発明では、コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報、及び複数種のアプリケーション・システムのうち個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第1権限情報が第1記憶手段に記憶されており、確認・許可手段は、コンピュータ・システムへのユーザのログイン要求に対し、第1記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、第1権限情報に基づきユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可する。

【0012】なお、ユーザ情報としては、例えばユーザIDとパスワード等の情報を適用することができる。また、ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可することは、例えば請求項2に記載したように、ユーザが個々のアプリケーション・システムの利用を要求するためのメニュー画面に、正当な利用者であることを確認できたユーザが利用権限を有しているアプリケーション・システムのみを選択肢として表示させることによって実現できるが、他の方法を用いてもよい。

【0013】第1権限情報は個々のアプリケーション・システムを単位とする個々のユーザの利用権限を表す情報であり、ユーザ情報についても個々のユーザを単位とする情報であるので、第1記憶手段に記憶されるこれらの情報のデータ構造は何れも簡単である。従って、本発明に係るコンピュータ・システムを利用可能なユーザを新規追加したり、或いはアプリケーション・システムを新規追加する等を目的とした情報の書き替えも容易であり、メンテナンス性に優れている。

【0014】また請求項1記載の発明では、複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して第2記憶手段が設けられており、この第2記憶手段には、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有している機能を特定するための第2権限情報が記憶されている。そして、第2記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、対応する第

2 記憶手段に記憶されている第2 権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供する。これにより、個々のユーザ毎に定められた利用権限（第1 権限情報及び第2 権限情報によって規定される利用権限）に従って、個々のユーザによるシステムの利用をコントロールすることができる。

【0015】なお、第2 記憶手段が設けられているアプリケーション・システムが、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、該ユーザが利用権限を有している機能のみをユーザに提供することは、例えば請求項3に記載したように、前記ユーザに対し、前記提供可能な機能の利用をユーザが要求するための画面に、前記ユーザが利用権限を有している機能のみを選択肢として表示させるか、又は、前記ユーザが利用権限を有していない機能の利用が前記ユーザから要求された場合に利用権限外であることを報知することによって実現できるが、他の方法を用いてもよい。

【0016】第2 権限情報は、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システム固有の権限情報であるので、アプリケーション・システムが提供する機能の種類等に応じて情報の体系が相違することになり、例えば請求項4に記載したように、対応するアプリケーション・システムがユーザに提供可能な機能についてのユーザの利用権限のレベルを複数のクラスに分類したときに、前記アプリケーション・システムの利用権限を有する個々のユーザが前記複数のクラスの何れに属するかを表す情報である場合もあれば、対応するアプリケーション・システムがユーザに提供可能な全機能について、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有するか否かを各々表す情報である場合もある。

【0017】これに対して請求項1記載の発明では、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でないアプリケーション・システムの各々に対応して第2 記憶手段が設けられているので、個々の第2 記憶手段に記憶されている第2 権限情報は、全てのアプリケーション・システムの第2 権限情報を統合した場合と比較して、データ構造が簡単になる。従って、特定のアプリケーション・システムに対応する第2 権限情報の情報体系を変更する等を目的とした第2 権限情報の書き替えも容易であり、メンテナンス性に優れている。

【0018】また、請求項1記載の発明において、特定のアプリケーション・システムが提供する特定の機能を特定ユーザが利用することは、第1 記憶手段に記憶されている第1 権限情報が、前記特定ユーザが前記特定のアプリケーション・システムの利用権限を有していることを表す内容となっており、かつ前記特定のアプリケーション・システムに対応する第2 記憶手段に記憶されてい

る第2 権限情報が、前記特定ユーザが前記特定の機能の利用権限を有していることを表す内容となっていることで初めて可能になる。このように、請求項1記載の発明では、個々のユーザの利用権限を規定する情報が第1 記憶手段と第2 記憶手段に分散されて管理されているので、セキュリティ性にも優れている。

【0019】従って、請求項1記載の発明によれば、個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メンテナンス性やセキュリティ性を損なうことなく実現することができる。

【0020】請求項5記載の発明は、請求項1記載の発明において、第2 記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な複数種の機能のうちの何れかの機能の利用がユーザから要求される毎に、利用が要求されている機能の利用権限をユーザが有しているか否かを判断することを特徴としている。

【0021】請求項5記載の発明では、第2 記憶手段が設けられているアプリケーション・システムが、提供可能な複数種の機能のうちの何れかの機能の利用がユーザから要求される毎に、利用が要求されている機能の利用権限を前記ユーザが有しているか否かを判断するので、アプリケーション・システムが提供可能な機能に対するユーザの利用権限を、各アプリケーション・システムが提供可能な個々の機能を単位として管理することが可能となり、各アプリケーション・システムが提供可能な個々の機能が、利用権限のないユーザによって不正に利用されることを確実に阻止することができる。

【0022】請求項6記載の発明は、請求項1記載の発明において、前記確認・許可手段は、正当な利用者であることを確認できたユーザに対し、前記ユーザが利用権限を有するアプリケーション・システムを前記ユーザが利用する際に用いるためのチケット情報を与え、前記複数種のアプリケーション・システムの各々は、自システムがユーザに提供可能な機能の利用を要求しているユーザが正当なチケット情報を所持しているか否かを判断することで、前記利用を要求しているユーザが自システムの利用権限を有している正当な利用者か否かを判定することを特徴としている。

【0023】請求項6記載の発明では、正当な利用者であることを確認できたユーザにチケット情報を与え、複数種のアプリケーション・システムの各々は、ユーザが正当なチケット情報を所持しているか否かを判断することで、前記ユーザが正当な利用者か否かを判定するので、正当なチケット情報を所持していないユーザが、利用権限を有していない特定のアプリケーション・システムに直接アクセスし、該特定のアプリケーション・システムが提供する機能を不正に利用しようとした場合にも、これを阻止することができる。従って、請求項6記

載の発明によれば、確認・許可手段による正当な利用者であることの確認を経ることなく、コンピュータ・システムが不正利用されることを阻止することができる。

【0024】なお、請求項6記載の発明において、確認・許可手段は、例えば請求項7に記載したように、チケット情報として、所定の情報を秘密鍵によって暗号化した情報を用いることができる。この場合、複数種のアプリケーション・システムの各々は、ユーザから端末を介して送信されたチケット情報を公開鍵によって復号化した際に所定の情報が再現されるか否かに基づいて、ユーザが正当なチケット情報を所持しているか否かを判断することができる。

【0025】請求項8記載の発明は、請求項6記載の発明において、確認・許可手段に異常が生じた場合に、コンピュータ・システムへのユーザのログイン要求に対し、前記ユーザのユーザIDを付加することで、前記ユーザがアプリケーション・システムを利用する際に使用可能な障害用チケット情報をユーザに与える障害チケット提供手段を更に備えたことを特徴としている。

【0026】本発明において、確認・許可手段として機能するコンピュータに何らかの異常が発生した等の理由により確認・許可手段に異常が生じ、コンピュータ・システムへのログイン要求が正常に受け付けられなくなった場合、各アプリケーション・システム自体は利用可能な状態であっても、正当な利用者が全てのアプリケーション・システムを利用できない状態に陥る、という不都合がある。これに対して請求項8記載の発明では、確認・許可手段に異常が生じた場合に、障害チケット提供手段によって障害用チケット情報がユーザに与えられるので、確認・許可手段に異常が生じた場合にも、正当な利用者が全てのアプリケーション・システムを利用できない状態に陥ることを回避することができる。

【0027】請求項9記載の発明に係るユーザ管理方法は、ユーザによって操作される端末と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システムに適用可能なユーザ管理方法であって、前記コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、前記複数種のアプリケーション・システムのうち前記個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第1権限情報を第1記憶手段に記憶しておくと共に、前記複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して設けられた第2記憶手段に、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限

を有している機能を特定するための第2権限情報を記憶しておき、前記コンピュータ・システムへのユーザのログイン要求に対し、前記第1記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、前記第1権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてののみ利用を許可し、前記第2記憶手段が設けられているアプリケーション・システムに対し、ユーザより前記アプリケーション・システムが提供可能な機能の利用が要求された場合に、対応する第2記憶手段に記憶されている第2権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供することを特徴としているので、請求項1記載の発明と同様に、個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メンテナンス性やセキュリティ性を損なうことなく実現できる。

【0028】

【発明の実施の形態】以下、図面を参照して本発明の実施形態の一例を詳細に説明する。図1には、金融機関の各種業務を支援するために金融機関に設置されたコンピュータ・システム10（以下、MIシステム10と称する）が示されている。

【0029】MIシステム10は、金融機関の各部署に設置された多数台のクライアントPC12（本発明の端末に相当）と、複数台のアプリケーション・サーバ14と、運用管理サーバ16と、障害用サーバ18が、イントラネット20を介して相互に接続されて構成されている。なお、アプリケーション・サーバ14、運用管理サーバ16及び障害用サーバ18は、請求項1に記載のコンピュータに各々対応している。

【0030】各アプリケーション・サーバ14は、各々ワークステーション又は汎用の大型コンピュータから成り、CPU14A、ROM14B、RAM14C、入出力ポート14Dを備え、これらがアドレスバス、データバス、制御バス等のバス14Eを介して互いに接続されて構成されている。入出力ポート14Dには、各種の入出力機器として、イントラネット20に接続された通信制御装置（例えばルータ）22、ディスプレイ24、マウス26、キーボード28、HDD30、及びCD-ROMからの情報の読み出しを行うCD-ROMドライブ32が各々接続されている。

【0031】金融機関では、業務の効率向上・顧客へのサービス向上を目的として、かなり以前より業務の機械化に取り組んでいるが、金融機関における業務は多種多様であるために、互いに異なる業務を支援するための互いに独立した複数種のアプリケーション・システムが存在していた。各アプリケーション・サーバ14は、元々は個々のアプリケーション・システムを実現するために、個々のアプリケーション・システムに対応して設け

(7)

特開2003-67336

11

られたコンピュータであり、各アプリケーション・サーバ14のHDD30には、対応する特定業務を支援する処理（アプリケーション処理）をCPU14Aによって実行するための互いに異なるアプリケーション・プログラムが予めインストールされている。

【0032】本実施形態に係るMIシステム10は、各アプリケーション・サーバ14によって実現される複数種のアプリケーション・システムを統合することで構築されたシステムであり、MIシステム10のユーザは、イントラネット20に接続された単一のクライアントP

10

C12を介してMIシステム10にログインすることで、任意のアプリケーション・システムが提供する任意の機能を利用することも可能に構成されている。

【0033】但し、MIシステム10では、各アプリケーション・システムがユーザに提供可能な各機能のうち、個々のユーザの業務に必要な機能についてのみ個々のユーザに利用権限を与えている。具体的には、MIシステム10への個々のユーザのログインの管理、及び、MIシステム10が提供可能な各機能についての個々のユーザの利用権限の管理の一部（個々のアプリケーション・システムを単位とする個々のユーザの利用権限の管理）は運用管理サーバ16によって行われる。なお、個々のアプリケーション・システムの利用に際してのより細かな利用権限の管理は個々のアプリケーション・システム（個々のアプリケーション・サーバ14）で行われる。

【0034】運用管理サーバ16はワークステーション又は汎用の大型コンピュータから成り、CPU16A、ROM16B、RAM16C、入出力ポート16Dを備え、これらがアドレスバス、データバス、制御バス等のバス16Eを介して互いに接続されて構成されている。入出力ポート16Dには、各種の入出力機器として、ディスプレイ36、マウス38、キーボード40、イントラネット20に接続された通信制御装置（例えばルータ）42、HDD44、及びCD-ROMからの情報の読み出しを行うCD-ROMドライブ46が各々接続されている。運用管理サーバ16には、MI運用管理処理（詳細は後述）を運用管理サーバ16のCPU16Aによって実行するためのMI運用管理プログラムがHDD44にインストールされている。

30

【0035】障害用サーバ18は、運用管理サーバ16と同様にワークステーション又は汎用の大型コンピュータから成るコンピュータであり、運用管理サーバ16に障害が発生し、MIシステム10へのログインが困難となった場合に、ユーザがMIシステム10にログインするための処理を運用管理サーバ16に代って行う。

【0036】また、クライアントPC12はパーソナル・コンピュータ（PC）から成り、CPU12A、ROM12B、RAM12C、入出力ポート12Dを備え、これらがアドレスバス、データバス、制御バス等のバス

50

12

12Eを介して互いに接続されて構成されている。入出力ポート12Dには、各種の入出力機器として、イントラネット20に接続された通信制御装置（例えばルータ）52、ディスプレイ54、マウス56、キーボード58、HDD60、及びCD-ROMからの情報の読み出しを行うCD-ROMドライブ62が各々接続されている。クライアントPC12には、MIシステム利用処理（詳細は後述）をクライアントPC12のCPU12Aによって実行するためのMIシステム利用プログラムがHDD60にインストールされている。

【0037】次に本実施形態の作用として、まず権限情報の登録について説明する。運用管理サーバ16のHDD44には、MIシステム10への個々のユーザのログインの管理及び個々のアプリケーション・システムを単位とする個々のユーザの利用権限の管理を行うためのユーザ情報データベース（DB）が記憶されている。このユーザ情報DBには、個々のユーザについて、例えば次の表1に示すような情報が記憶されている。

【0038】

【表1】

< ユーザ情報DBの内容(一例) >

| 項目 | 内容 |
|------------------|----------|
| ユーザID | xxxxxxx |
| パスワード | yyyyyyyy |
| 所属部署ID | zzzz |
| 役職ID | www |
| その他の属性情報 | vvvv |
| 利用権限を有するアプリケーション | アプリA |
| | アプリB |
| | ; |

【0039】表1において、「ユーザID」はMIシステム10の利用権限を有する個々のユーザを識別するための情報であり、「パスワード」はログインに際してユーザ認証に用いる情報、「所属部署ID」「役職ID」及び「その他の属性情報」は個々のユーザの所属部署、役職やその他（例えば個々のユーザが行う業務の管理区分等）を識別するための情報である。また、本実施形態に係るMIシステム10では、個々のユーザに対し、個々のユーザの業務の遂行に必要なアプリケーション・システムについてのみ利用権限を与えている。このため「利用権限を有するアプリケーション」には、個々のユーザが利用権限を有しているアプリケーション・システムのIDが登録設定される。ユーザ情報DBへの個々のユーザの情報の登録は、MIシステム10全体を管理している部署で行われる。

【0040】なお、上述した各種の情報のうち、「利用権限を有するアプリケーション」は本発明の第1権限情報に、それ以外の情報は本発明のユーザ情報に各々対応しており、ユーザ情報DBを記憶するHDD44は本発

(8)

特開2003-67336

13

明の第1記憶手段に対応している。表1からも明らかなように、ユーザ情報DBにはアプリケーション・システムを単位とする各ユーザの利用権限のみが記憶されているので、ユーザ情報DBに記憶されている情報はデータ構造が非常に簡単であり、利用ユーザを追加したり、新たなアプリケーション・システムが追加された場合に情報を更新する等のメンテナンスを簡単に行うことができる。

【0041】また、各アプリケーション・サーバ14のHDD30には、個々のユーザが対応するアプリケーション・システムを利用するに際し、より細かな利用権限の管理を行うために、個々のユーザの利用権限を特定するための情報が登録された権限情報DBが記憶されている。なお、権限情報DBは本発明の第2権限情報に対応しており、権限情報DBを記憶する各アプリケーション・サーバ14のHDD30は本発明の第2記憶手段に対応している。この権限情報DBの内容（利用権限を規定する情報の体系）は個々のアプリケーション・システム（個々のアプリケーション・サーバ14）によって相違している。

【0042】すなわち、本実施形態では、各アプリケーション・サーバ14によって実現される各アプリケーション・システムの中に、日本銀行の当座預金や国債の決済に関する業務を支援するためのアプリケーション・システム（以下、RTGSシステムという）が含まれている。このRTGSシステムでは、例として次の表2に示すように、ユーザに与える利用権限が2次元のマトリックスを用いてユーザの所属部署及び役職毎に予めパターン化されており、所属部署及び役職毎に定められた利用権限のパターンは権限パターン情報としてRTGSシステムの権限情報DBに記憶されている。

【0043】

【表2】

＜RTGSシステムにおける利用権限のパターン＞

| | 部署A | | 部署B | | ... |
|-----|-----|-----|-----|-----|-----|
| | 役職A | 役職B | 役職A | 役職B | ... |
| 機能a | | ○ | | ○ | ... |
| 機能b | ○ | ○ | | ● | ... |
| 機能c | ● | ○ | ○ | ○ | ... |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

【0044】但し、「●」は参照のみ可、「○」は参照及び更新可

従って、RTGSシステムでは所属部署及び役職が同一のユーザに同一の利用権限が与えられるので、RTGSシステムを利用する個々のユーザに対する利用権限の設定は、図2に例として示すユーザ情報設定画面からも明

14

らかなように、所属部署（図2では「部署名」及び「グループ」）、役職（図2では「権限」）、ユーザID（ログインID）等の情報を入力することで完了し、RTGSシステムの権限情報DBには、個々のユーザの利用権限が何れのパターンに対応しているかを特定するための情報（例えば所属部署IDと役職ID等）がユーザIDと対応されて記憶される。

【0045】また、MIシステム10の各アプリケーション・システムの中には、円資金に関する業務を支援するためのアプリケーション・システム（以下、RAPIDシステムという）が含まれている。このRAPIDシステムでは、ユーザの所属部署及び役職と無関係に、利用権限のパターンを任意に作成可能とされている。

【0046】すなわち、例として図3に示すRAPIDシステムの権限パターン設定画面は、画面右側に機能名称表示欄70が設けられており、この機能名称表示欄70に一覧表示された機能の中から特定の機能を選択することで、選択した機能の利用権限が作成中の利用権限のパターンに付加される。作成された利用権限のパターンは、権限パターン設定画面の左側に設けられたパターン番号入力欄72に設定されたパターン番号がIDとして付加され、権限パターン情報としてRAPIDシステムの権限情報DBに記憶される。

【0047】そして、RAPIDシステムを利用する個々のユーザに対する利用権限の設定は、例として図4に示すユーザ情報設定画面からも明らかなように、ユーザIDや所属部署、役職等の情報に加え、該ユーザに設定する利用権限のパターンを設定欄74にパターン番号（ID）で設定することで完了し、RAPIDシステムの権限情報DBには、個々のユーザの利用権限が何れのパターンに対応しているかを特定するためのパターンID等の情報がユーザIDと対応されて記憶される。なお、RAPIDシステムでは利用権限のパターンをユーザの所属部署及び役職と無関係に作成できるので、必要に応じて個々のユーザ毎にパターンを作成することも可能であり、個々のユーザの利用権限をより細かく設定することができる。

【0048】また、各アプリケーション・システムの中には、デリバティブに関する業務を支援するためのアプリケーション・システム（以下、PYRAMIDシステムという）が含まれている。このPYRAMIDシステムでは、ユーザに与える利用権限として、次の表3に示すような複数のカテゴリが存在しており、利用権限の規定方法は各カテゴリ毎に相違している。

【0049】

【表3】

| 権限の種類 | 権限の内容 |
|-------------------|--------------------|
| オペレーション権限 | 各種オペレーション画面を操作する権限 |
| 取引オペレーション権限 | 約定データに対するオペレーション権限 |
| マーケットデータオペレーション権限 | マーケットデータを登録/更新する権限 |
| ： | ： |

【0050】例えば表3に示した各カテゴリのうち、「オペレーション権限」については、アシスタント／ディーラー／チーフの各役職に対応する3つのオペレーション権限クラスについて、「オペレーション権限」に属する各種機能の利用権限が各々パターン化されており、個々のオペレーション権限クラス毎の各種機能の利用権限のパターンは、オペレーション権限パターン情報としてPYRAMIDシステムの権限情報DBに記憶されている。

【0051】PYRAMIDシステムを利用する個々のユーザに対する「オペレーション権限」に関する利用権限の設定は、個々のユーザが3つのオペレーション権限クラスのうちの何れのクラスに属するかを指定することによって行われ、指定したオペレーション権限クラスがユーザIDと対応されてPYRAMIDシステムの権限情報DBに記憶されることにより、個々のユーザの「オペレーション権限」に属する各種機能の利用権限（各種オペレーション画面を操作（参照のみ／参照及び更新）する権限）が登録される。

【0052】また「取引オペレーション権限」については、アシスタント／ディーラー／チーフの各役職に対応する3つの取引オペレーション権限クラスについて、「取引オペレーション権限」に属する各種機能の利用権限が各々パターン化されていると共に、「取引オペレーション権限」に関連する利用権限（例えば取扱可能な通貨権限や取扱可能な商品権限等）が、所属部署及び個々のユーザが行う業務の管理区分を単位として定められており、個々の取引オペレーション権限クラス毎の利用権限のパターン、所属部署及び管理区分を単位とする利用権限は、取引オペレーション権限情報としてPYRAMIDシステムの権限情報DBに記憶されている。

【0053】このため「取引オペレーション権限」に関しては、PYRAMIDシステムを利用する個々のユーザが3つの取引オペレーション権限クラスのうちの何れのクラスに属するかを指定すると共に、所属部署及び管理区分を指定することによって行われ、指定した取引オペレーション権限クラス、所属部署及び管理区分がユーザIDと対応されてPYRAMIDシステムの権限情報DBに記憶されることにより、個々のユーザの「取引オペレーション権限」に属する各種の利用権限（約定データに対する各種のオペレーション権限）が登録される。

【0054】このように、各アプリケーション・システムが提供可能な各種機能を単位とする各ユーザの細かな利用権限については、対応する各アプリケーション・サ

ーバ14のHDD30に記憶され、アプリケーション・システム毎に分離されているので、MIシステム10に関する各ユーザの利用権限を一元管理する場合と比較して、利用権限を規定する情報（各アプリケーション・サーバ14の権限情報DBに記憶する情報）のデータ構造が簡単になると共に、他のアプリケーション・システムの影響を受けることなく利用権限を規定する情報の体系を自由に定めることができる。従って、利用ユーザの追加等のメンテナンスや利用権限を規定する情報の体系そのものの変更等も比較的簡単に行うことができる。

【0055】続いて図5～図7のフローチャートを参照し、ユーザがMIシステム10を利用する際に各コンピュータで実行される処理について説明する。ユーザがクライアントPC12に対してMIシステム10の利用を指示すると、MIシステム利用プログラムがクライアントPC12のCPU12Aによって実行されることにより、図5に示すMIシステム利用処理がクライアントPC12で実行される。

【0056】このMIシステム利用処理では、まずステップ100において、例として図8に示すようなMIログイン画面をクライアントPC12のディスプレイ54に表示することで、MIシステム10にログインするためのユーザID及びパスワードの入力をユーザに要請する。次のステップ102ではユーザからログインの実行が指示されたか判定し、判定が肯定される迄待機する。

【0057】MIログイン画面には、ユーザIDを入力するための入力欄76、パスワードを入力するための入力欄78及びログインの実行を指示するためのボタン80が設けられている。ユーザがクライアントPC12のキーボード58やマウス56を操作することで、入力欄76にユーザIDを、入力欄78にパスワードを各々入力し、更にボタン80をクリックすると、ステップ102の判定が肯定されてステップ104へ移行し、入力されたユーザID及びパスワードをイントラネット20を介して運用管理サーバ16へ送信することで、MIシステム10へのログインを要求する。ステップ106では、ログイン要求に対する応答を運用管理サーバ16から受信したか否か判定し、判定が肯定される迄待機する。

【0058】一方、運用管理サーバ16では、CPU16AによってMI運用管理プログラムが実行されることで、図6に示すMI運用管理処理が常時実行されている。このMI運用管理処理では、ステップ170でクライアントPC12等の他のコンピュータから何らかの要

(10)

特開2003-67336

17

求を受信したか否か判定し、判定が肯定される迄待機する。ステップ170の判定が肯定されるとステップ172へ移行し、他のコンピュータから受信した要求の内容を判定し、判定結果に応じて分岐する。

【0059】受信した要求が前述のようなクライアントPC12からのログイン要求であった場合には、ステップ172からステップ174へ移行する。なお、ステップ174～ステップ190は本発明の確認・許可手段に対応している。

【0060】すなわち、ステップ174では、クライアントPC12から受信したユーザID及びパスワードをキーにしてユーザ情報DBを検索する。また、次のステップ176では、ステップ174の検索の結果に基づき、受信したユーザIDとパスワードの組み合わせがユーザ情報DBに登録されているか否かを判定する。この判定が否定された場合には、今回のログイン要求がMIシステム10の正当なユーザからの要求ではないと判断できるのでステップ190へ移行し、ログイン要求元のクライアントPC12に対し、ユーザID未登録やパスワード誤り等の理由でログインを受け付けできない旨を通知するエラー応答を送信した後にステップ170に戻る。

【0061】また、ステップ176の判定が肯定された場合には、ユーザID及びパスワードと対応付けられてユーザ情報DBに記憶されている情報（所属部署IDや役職ID等）をユーザ情報DBから読み出してRAM16C等に一時記憶した後にステップ178へ移行し、受信したユーザIDをキーにしてログイン管理テーブルを検索する。また、ステップ180ではステップ178の検索の結果に基づき、受信したユーザIDがログイン管理テーブルに登録されているか否か判定する。

【0062】このログイン管理テーブルは、MIシステム10に現在ログインしている全ユーザのユーザIDを登録するテーブルであり、ステップ180の判定が肯定された場合には二重ログインであると判断できるので、ステップ190において、ログイン要求元のクライアントPC12に対して二重ログインを通知するエラー応答を送信した後にステップ170に戻る。また、ステップ180の判定が否定された場合には、要求されているログインは正当なユーザからの正当なログイン要求であると判断し、ステップ182において、先に受信したユーザIDをログイン日時等の情報と対応付けてログイン管理テーブルに追加登録する。

【0063】次のステップ184では、ユーザ情報DBから読み出して一時記憶している情報及びユーザIDに基づいて、ログインするユーザが利用権限の有るアプリケーション・システムを利用する際に必要となるチケットを生成する。具体的には、例えばユーザID等のユーザに関する情報に、チケット発行日時や、ユーザが知り得ない所定のマジックワード（例えばバージョン情報）

18

等を付加した後に、一連の情報を秘密鍵によって暗号化することによって生成することができる。

【0064】また、ステップ186ではユーザ情報DBから読み出して一時記憶している権限情報（「利用権限を有するアプリケーション」）に基づき、ログイン要求元のクライアントPC12のディスプレイ54に表示するMIメニュー画面（一例を図9に示す）を規定するメニュー定義情報を生成する。

【0065】図9は、MIシステム10の各アプリケーション・システムのうち、RTGSシステム及びRAPIDシステムについてのみ利用権限を有しているユーザがログインした際に表示されるMIメニュー画面が示されている。図9からも明らかなように、本実施形態に係るMIメニュー画面には、MIシステム10に含まれる各アプリケーション・システムの名称が記されたボタン82A～82Gが設けられているが、ユーザが利用権限を有しているアプリケーション・システムのボタン82（図9の例ではボタン82C、82D）についてのみ、ユーザが利用対象として選択可能なようにアクティブ表示され、ユーザが利用権限を有していないアプリケーション・システムに対応するボタン82は非アクティブ表示されることで、利用対象として選択できないようになっている。

【0066】ステップ186では、メニュー定義情報に基づいて上記のようなMIメニュー画面がクライアントPC12のディスプレイ54に表示されるように、メニュー定義情報を生成する。なお、上記のように非アクティブ表示することに代えて、ユーザが利用権限を有していないアプリケーション・システムに対応するボタン82を表示しないようにしてもよい。

【0067】そして次のステップ188では、生成したチケット及びメニュー定義情報をログイン要求元のクライアントPC12へ送信することで、ログイン要求に対して正常応答を返し、ステップ170に戻る。

【0068】MIシステム利用処理（図5）では、ステップ104でログインを要求してから所定時間以内に運用管理サーバ16から何らかの応答を受信するか、又は運用管理サーバ16からの応答がタイムアウトになると、ステップ108において、運用管理サーバ16から正常な応答を受信したか否か判定する。

【0069】運用管理サーバ16からエラー応答を受信した場合、或いは運用管理サーバ16からの応答がタイムアウトになった場合には、判定が否定されてステップ112へ移行し、ディスプレイ54にエラー画面を表示することで、MIシステム10への通常のログインに失敗したことをユーザに通知する。そして、運用管理サーバ16からのエラー応答を受信している場合には、受信したエラー応答に基づき、ユーザID未登録やパスワード誤り等の理由でログインを受け付けできない旨を通知するメッセージを表示したり、或いは二重ログインであ

(11)

特開2003-67336

19

20

ることを通知するメッセージを表示する。

【0070】次のステップ114では運用管理サーバ16からの応答がタイムアウトになったか否かに基づいて、運用管理サーバ16に障害が発生しているか否かを判定する。判定が否定された場合にはステップ102に戻り、ユーザID及びパスワードが入力されてログインの実行が再度指示される迄待機する。なお、ステップ114の判定が肯定された場合の処理については後述する。

【0071】また、運用管理サーバ16から正常な応答を受信した場合には、ステップ108の判定が肯定されてステップ110へ移行し、運用管理サーバ16から受信したチケット及びメニュー定義情報をHDD60に記憶する。次のステップ122では、HDD60に記憶したメニュー定義画面に基づいて、前述したMIメニュー画面（図9参照）をディスプレイ54に表示する。

【0072】前述のように、MIメニュー画面は、ユーザが利用権限を有していないアプリケーション・システムは利用対象として選択できないようになっているので、利用権限を有していないアプリケーション・システムをユーザが利用することを阻止することができる。また、複数のアプリケーション・システムの利用権限を有しているユーザが、利用権限を有している複数のアプリケーション・システムを順次又は並列に利用する場合にも、ユーザID及びパスワードを入力しログインを指示する、というログイン動作を1回行うのみで、単一のクライアントPC12から複数のアプリケーション・システムを利用することが可能となり、シングル・サインオンを実現できる。

【0073】ステップ124では、MIメニュー画面内の何れかのボタンが選択されたか否かを判定し、判定が肯定される迄待機する。オペレータがマウス56等を操作してMIメニュー画面内の何れかのボタンを選択すると、ステップ124の判定が肯定されてステップ126へ移行し、ユーザによって選択されたボタンが、ボタン82A～82Gのうちアクティブ表示されている特定のボタン82か否かに基づいて、利用権限を有する特定のアプリケーション・システムの利用がユーザによって選択されたか否かを判定する。

【0074】ステップ126の判定が肯定された場合にはステップ128へ移行し、HDD60に記憶しているチケットを読み出し、読み出したチケットにユーザによる操作の内容を表す情報等を付加し、ユーザによって選択されたボタン82に対応する特定のアプリケーション・サーバ14へ送信することで、対応する特定のアプリケーション・システムが提供する各種機能のうち、ユーザの指示に対応する特定機能（例えばMIメニュー画面上の対応するボタン82がユーザによって選択された場合には、特定のアプリケーション・システムのメインメニューをディスプレイ54に表示させる機能）の利用を

要求する。次のステップ130では、チケット送信先のアプリケーション・サーバ14から何らかの応答を受信したか否かを判定し、判定が肯定される迄待機する。

【0075】一方、各アプリケーション・サーバ14では、HDD30にインストールされているアプリケーション・プログラムがCPU14Aによって実行されることで、図7に示すMIアプリケーション処理が各々実行されている。MIアプリケーション処理では、ステップ210でクライアントPC12から特定機能の利用を要求する情報を受信したか否かを判定し、判定が肯定される迄待機する。

【0076】本実施形態において、例えばRTGSシステムが提供する特定機能を利用することは、MIメニュー画面上のRTGSシステムに対応するボタン82Cを選択し、RTGSシステムに対応するアプリケーション・サーバ14により、例として図10に示すようなRTGSシステムのメニューバーがディスプレイ54に表示されている状態で、プルダウンメニューを表示させて所望の項目を選択することによって成される。

【0077】また、例えばRAPIDシステムが提供する特定機能を利用することは、MIメニュー画面上のRAPIDシステムに対応するボタン82Dを選択し、RAPIDシステムに対応するアプリケーション・サーバ14により、例として図11に示すようなRAPIDシステムのメインメニュー画面がディスプレイ54に表示されている状態で、所望の項目を順次選択することによって成される。

【0078】ここで、図10や図11に示すメニューをディスプレイ54に表示させることを含め、特定のアプリケーション・システムの特定機能を利用することは、詳しくは、特定機能の利用を要求する操作をユーザが行う毎に、ユーザの操作に応じてクライアントPC12から対応するアプリケーション・サーバ14へ特定機能の利用を要求する情報が送信され（前述したステップ128）、情報を受信したアプリケーション・サーバ14が、図7のステップ210の判定が肯定されることでステップ212以降を実行することによって実現される。

【0079】図7のフローチャート（のステップ212）は、特定機能の利用を要求する情報をクライアントPC12から受信する毎に個々のアプリケーション・サーバ14で実行される処理のうちの共通する部分について説明するフローチャートであり、以下では、情報を受信したアプリケーション・サーバ14（アプリケーション・システム）及び利用が要求された機能を明記することなくステップ212以降を説明するが、実際の処理（例えば後述するステップ220に相当する処理の内容等）は、情報を受信したアプリケーション・サーバ14（アプリケーション・システム）及び利用が要求された機能によって大きく相違していることを付記しておく。

【0080】ステップ212では、クライアントPC1

(12)

特開2003-67336

21

2から受信した情報に含まれるチケットを抽出し、抽出したチケットに基づいて、要求元のクライアントPC12を操作しているユーザの認証を行う。このユーザ認証は、受信したチケットが運用管理サーバ16によって発行された正当なチケットか否かを判断することで行うことができ、具体的には、例えば運用管理サーバ16が暗号化に用いた秘密鍵に対応する公開鍵を用いてチケットを復号化し、復号化によって得られた一連の情報に含まれているユーザIDがHDD30に記憶されている権限情報DBに登録されているか否かを照合すると共に、前記一連の情報に含まれているマジックワードを正規のマジックワードと照合することで行うことができる。

【0081】なお、運用管理サーバ16によって発行されたチケットには有効期限が設けられている。本実施形態では、チケットの有効期限を「運用管理サーバ16によってチケットが発行されてから24時間未満」としている。チケットを復号化することで得られる一連の情報にはチケット発行日時が含まれており、ステップ212では、チケット発行日時からの経過時間が24時間未満か否かも判定し、24時間以上経過していた場合には正当なチケットではないと判断する。この場合、ユーザは、MIシステム10から一旦ログアウトした後に再度ログインすることで、チケットを再度取得する必要がある。

【0082】ステップ214では、ステップ212における認証の結果に基づいて、クライアントPC12を介して特定機能の利用を要求しているユーザが、対応するアプリケーション・システムの利用権限を有する正当なユーザか否かを判定する。受信したチケットが運用管理サーバ16によって発行された正当なチケットではないと判断された場合には、ステップ214の判定が否定されてステップ230へ移行し、要求元のクライアントPC12に対して、ユーザが対応するアプリケーション・システムの利用権限を有していない旨を通知するエラー応答を返し、ステップ210に戻る。

【0083】仮に、所望のアプリケーション・システムが提供する所望の機能を不正に利用しようと目論む者が、クライアントPC12からアプリケーション・サーバ14に直接アクセスするための手段を知り得たとしても、上述のように、正当なチケットを所有していなければエラーとなり、そしてチケットを偽造することは極めて困難であるので、アプリケーション・システム側でチケットによるユーザ認証を行うことにより、MIシステム10にログインすることなくMIシステム10を不正に利用することを阻止することができる。

【0084】一方、受信したチケットが運用管理サーバ16によって発行された正当なチケットであると判断された場合にはステップ216へ移行し、前記一連の情報に含まれるユーザIDを用いて権限情報DBを検索することで、特定機能の利用を要求しているユーザに対応す

22

る情報を抽出する。そして、次のステップ218において、ステップ216の検索によって抽出された情報に基づいて、特定機能の利用を要求しているユーザが特定機能の利用権限を有しているか否かを判定する。

【0085】例えばRTGSシステムでは、所属部署及び役職毎に利用権限のパターンが定められており、RTGSシステムの利用権限を有する個々のユーザの利用権限が何れのパターンに対応しているかを特定するための情報が、個々のユーザのユーザIDと対応付けられてRTGSシステムの権限情報DBに記憶されているので、利用権限の有無の判定は、例えば特定機能の利用を要求しているユーザのユーザIDに基づいて、該ユーザの利用権限を表す利用権限パターンを特定し、利用が要求されている特定機能が、前記特定した利用権限パターン上で「利用権限有り」になっているか否かを判断することによって成される。

【0086】また、例えばRAPIDシステムでは、利用権限のパターンがユーザの所属部署及び役職と無関係に作成されるが、RAPIDシステムの利用権限を有する個々のユーザの利用権限が何れのパターンに対応しているかを特定するための情報が、個々のユーザのユーザIDと対応付けられてRAPIDシステムの権限情報DBに記憶されているので、利用権限の有無の判定は、RTGSシステムと同様に、例えば特定機能の利用を要求しているユーザのユーザIDに基づいて、該ユーザの利用権限を表す利用権限パターンを特定し、利用が要求されている特定機能が、前記特定した利用権限パターン上で「利用権限有り」になっているか否かを判断することによって成される。

【0087】更に、例えばPYRAMIDシステムでは、ユーザに与える利用権限として複数のカテゴリ（表3参照）が存在しているので、利用権限の有無は、例えばユーザから利用を要求されている特定機能が何れのカテゴリに属する機能かを判断し、判断したカテゴリに応じた判定方法で判定される。

【0088】すなわち、「オペレーション権限」については、「オペレーション権限」に属する各種機能の利用権限がオペレーション権限クラス毎にパターン化されており、PYRAMIDシステムの利用権限を有する個々のユーザのオペレーション権限クラスがユーザIDと対応付けられてPYRAMIDシステムの権限情報DBに記憶されているので、ユーザから利用が要求された特定機能が「オペレーション権限」に属する機能であった場合、利用権限の有無の判定は、例えば特定機能の利用を要求しているユーザのユーザIDに基づいて、該ユーザのオペレーション権限クラスを特定し、利用が要求されている特定機能が、前記特定したオペレーション権限クラスに対応する利用権限パターン上で「利用権限有り」になっているか否かを判断することによって成される。

【0089】また「取引オペレーション権限」について

50

(13)

23

は、「取引オペレーション権限」に属する各種機能の利用権限が取引オペレーション権限クラス毎にパターン化されていると共に、「取引オペレーション権限」に関連する利用権限が所属部署及び管理区分を単位として定められており、PYRAMIDシステムの利用権限を有する個々のユーザの取引オペレーション権限クラス、所属部署及び管理区分が、ユーザIDと対応付けられてPYRAMIDシステムの権限情報DBに記憶されている。

【0090】このため、ユーザから利用が要求された特定機能が「取引オペレーション権限」に属する機能であった場合、利用権限の有無の判定は、例えば特定機能の利用を要求しているユーザのユーザIDに基づいて、該ユーザの取引オペレーション権限クラス、所属部署及び管理区分を各々特定し、利用が要求されている特定機能が、前記特定した取引オペレーション権限クラスに対応する利用権限パターン上で「利用権限有り」になっており、かつ特定した所属部署及び管理区分を単位とする利用権限でも利用権限内か否か（すなわち、取引オペレーション権限クラスによって規定される利用権限と所属部署及び管理区分によって規定される利用権限の論理積（AND））を判断することによって成される。

【0091】特定機能の利用を要求しているユーザが特定機能の利用権限を有していない場合には、ステップ218の判定が否定されてステップ230へ移行し、要求元のクライアントPC12に対して、利用が要求された特定機能はユーザの利用権限外である旨を通知するエラー応答を返し、ステップ210に戻る。

【0092】また、利用が要求されている特定機能の利用権限をユーザが有していた場合には、ステップ218の判定が肯定されてステップ220へ移行し、ユーザの要求に応じて特定機能を提供する処理を行う。この処理としては、例えばユーザがクライアントPC12のディスプレイ54への表示を要求した情報をHDD30等から読み出す処理、HDD30等に記憶されている情報のうちユーザが更新を指示した情報を更新する処理、ユーザの指示に応じて所定の演算を行う処理、ユーザの指示に応じて他のコンピュータへ所定の情報（電文）を送信する処理等が挙げられる。

【0093】ステップ222では、ステップ220で行った処理結果に基づき、該処理の結果を要求元のクライアントPC12のディスプレイ54に表示するための画面定義情報を生成する。次のステップ224では、ステップ222で生成した画面定義情報によって定義される画面内に、ユーザが利用権限を有していない項目（例えばユーザが利用権限を有していない機能を選択するためのボタン等）が有るか否かを判定する。

【0094】ステップ224の判定が肯定された場合にはステップ226へ移行し、前述のMIメニュー画面と同様に、ユーザが利用権限を有していない項目が非アクティブ表示になるように画面定義情報の内容を変更した

特開2003-67336

24

後にステップ228へ移行する。なお、非アクティブ表示にすることに代えて、ディスプレイ54に表示されないように画面定義情報の内容を変更するようにしてもよい。また、ステップ224の判定が否定された場合には、何ら処理を行うことなくステップ228へ移行する。そして、ステップ228では要求元のクライアントPC12へ画面定義情報等を送信し、ステップ210に戻る。

【0095】チケット等を送信したクライアントPC12が送信先のアプリケーション・サーバ14から何らかの応答を受信すると、MIシステム利用処理（図5）のステップ130の判定が肯定され、次のステップ132でアプリケーション・サーバ14からの応答が正常応答か否かを判定する。アプリケーション・サーバ14からの応答がエラー応答の場合には、前記判定が否定されてステップ136へ移行し、所定のエラー画面をディスプレイ54に表示すると共に、受信したエラー応答の内容に応じて、選択されたアプリケーション・システムはユーザの利用権限外である旨を通知するメッセージ、或いは、利用が要求された特定機能はユーザの利用権限外である旨を通知するメッセージを表示する。

【0096】また、アプリケーション・サーバ14からの応答が正常応答の場合には、ステップ132の判定が肯定されてステップ134へ移行し、アプリケーション・サーバ14から受信した画面定義情報に基づいて、先に特定機能を利用を要求したことに對するアプリケーション・サーバ14（アプリケーション・システム）の処理結果をディスプレイ54に表示する。これにより、ユーザが利用を要求した特定機能についての処理結果をユーザが参照又は確認することができる。

【0097】次のステップ138では、アプリケーション・システムが提供する他の特定機能の利用がユーザによって選択されたか否かを判定する。判定が否定された場合にはステップ140へ移行し、ユーザによってアプリケーション・システムの利用終了が選択されたか否かを判定する。この判定も否定された場合にはステップ138に戻り、何れかの判定が肯定される迄ステップ138、140を繰り返す。

【0098】例えばユーザがキーボード58やマウス56等を操作し、ディスプレイ54に表示された項目のうち、利用したい特定機能に対応する特定項目を選択すると、ステップ138の判定が肯定されてステップ128に戻り、上述したステップ128以降の処理が繰り返されることになる。これにより、ユーザはアプリケーション・システムが提供する各種機能のうち業務の遂行に必要な機能（自身が利用権限を有する機能）を利用しながら、業務を遂行することができる。ユーザによってアプリケーション・システムの利用終了が選択されると、ステップ140の判定が肯定されてステップ122に戻り、ディスプレイ54にMIメニュー画面が再度表示さ

れる。

【0099】ところで、MIメニュー画面（図9）には、利用するアプリケーション・システムを選択するためのボタン82の他に、パスワードを変更するためのボタン84と、MIシステム10からログアウトするためのボタン86も設けられている。また、図9では非アクティブ表示されているが、システム管理者がメンテナンス作業等を行うためのボタン88も設けられている。

【0100】ディスプレイ54にMIメニュー画面が表示されている状態で、ユーザによってボタン82以外のボタンが選択された場合には、ステップ122からステップ124、126を経てステップ142へ移行し、MIシステム10からのログアウトがユーザによって選択されたか否か判定する。

【0101】判定が否定された場合にはステップ150へ移行し、ユーザが選択したボタンに対応する処理（例えばパスワードを変更するための処理や、システム管理者がメンテナンス等の作業を行うための処理）の実行を運用管理サーバ16に要求する。これにより、運用管理サーバ16ではMI運用管理処理（図6）のステップ170、172を経てステップ198へ移行し、クライアントPC12からの要求に応じた処理を実行する。そして、ユーザが選択したボタンに対応する処理が完了すると、MIシステム利用処理（図5）のステップ150からステップ122に戻る。

【0102】また、MIシステム10からログアウトするためのボタン86がユーザによって選択された場合には、ステップ142からステップ144へ移行し、HDD60に格納していたチケットを廃棄する。ステップ146では、運用管理サーバにユーザIDを送信してMIシステム10からのログアウトを要求し、次のステップ148では応答を受信する迄待機する。

【0103】運用管理サーバ16では、クライアントPC12からログアウトが要求されると、MI運用管理処理（図6）のステップ170、172を経てステップ192へ移行する。ステップ192では、受信したユーザIDをキーにしてログイン管理テーブルを検索し、ステップ194ではステップ192における検索の結果に基づき、ログイン管理テーブルから該当情報（ユーザIDやログイン日時等）を削除する。そして、ログアウト要求元のクライアントPC12に対し、正常にログアウトできた旨を通知する応答を送信する。

【0104】この応答がログアウト要求元のクライアントPC12で受信されることで、MIシステム利用処理（図5）のステップ148の判定が肯定され、MIシステム利用処理の実行が終了する。

【0105】続いて、運用管理サーバ16の応答がタイムアウトになった場合（MIシステム利用処理（図5）のステップ114の判定が肯定された場合）の処理について説明する。本実施形態では運用管理サーバ16が二

重化されているので、運用管理サーバ16からの応答がタイムアウトになった場合は、運用管理サーバ16の両系共に障害が発生し応答を返すことができない状態であると判断できる。

【0106】このため、ステップ114の判定が肯定された場合にはステップ116へ移行し、ログインを要求しているユーザによって入力されたユーザID及びパスワードを障害用サーバ18へ送信することで、MIシステム10へのログインを要求する。次のステップ118では、障害用サーバ18から応答を受信したか否か判定し、判定が肯定される迄待機する。

【0107】本実施形態では障害用サーバ18にユーザ情報DBが設けられていないため、クライアントPC12からログインが要求されると、障害用サーバ18は障害時チケット（ユーザIDが未設定のチケット）を生成し、ログイン要求元のクライアントPC12へ送信する。障害用サーバ18に対してログインを要求したクライアントPC12は、障害用サーバ18から障害時チケットを受信すると、ステップ118の判定が肯定されてステップ120へ移行し、受信した障害時チケットにログインを要求しているユーザのユーザIDを設定し、HDD60に格納した後ステップ122へ移行する。

【0108】これにより、運用管理サーバ16に障害が発生し正規のチケットが発行されない場合にも、障害用サーバ18によって発行される障害時チケットを用いることで、MIシステム10の各アプリケーション・システムを利用することができる。また、運用管理サーバ16に障害が発生している際にも、各アプリケーション・システムにおいて、ユーザIDに基づく利用権限のチェックが行われるので、ユーザが利用権限外のアプリケーション・システムを利用したり、利用権限外の機能を利用することを阻止することができる。

【0109】なお、上記ではMIシステム10を利用するための専用プログラム（MIシステム利用プログラム）がクライアントPC12にインストールされており、このプログラムに従ってクライアントPC12がMIシステム利用処理を行うことで、MIシステム10の利用が可能となる場合を例に説明したが、本発明はこれに限定されるものではなく、例えばクライアントPC12にブラウザ等の一般的なプログラムのみがインストールされている環境下でも本発明は実現可能である。

【0110】また、上記ではMIシステム10に含まれる全てのアプリケーション・システムに各ユーザ毎の利用権限を規定する権限情報DBが設けられており、各アプリケーション・システムは、ユーザから特定機能の利用が要求される毎に、チケットを用いたユーザ認証を行うと共に、権限情報DBに基づきユーザが特定機能の利用権限を有しているか否かを判定する場合を説明したが、これに限定されるものではなく、本発明に係るコン

(15)

27

ビュータ・システムの中に、個々のユーザの利用権限が一定のアプリケーション・システム（例えば提供可能な全機能を全ユーザに提供するアプリケーション・システム）が含まれていてもよい。この場合、利用権限の判定は省略可能であるが、セキュリティ性確保のためにチケットを用いたユーザ認証は省略しないことが望ましい。

【0111】また、上記では金融機関のコンピュータ・システムに本発明を適用した例を説明したが、これに限定されるものではなく、本発明は、複数のアプリケーション・システムを含んで構成された任意のコンピュータ・システムに適用可能であることは言うまでもない。

【0112】

【発明の効果】以上説明したように請求項1及び請求項9記載の発明は、コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第1権限情報を第1記憶手段に記憶すると共に、アプリケーション・システムに対応して設けられた第2記憶手段に、対応するアプリケーション・システムが提供可能な複数種の機能のうち、個々のユーザが利用権限を有している機能を特定するための第2権限情報を記憶し、コンピュータ・システムへのユーザのログイン要求に対し、ユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、第1権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可し、アプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、第2権限情報に基づき、前記ユーザが利用権限を有している機能のみを前記ユーザに提供するので、個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メンテナンス性やセキュリティ性を損なうことなく実現できる、という優れた効果を有する。

【0113】請求項5記載の発明は、請求項1記載の発明において、アプリケーション・システムは、提供可能な複数種の機能のうちの何れかの機能の利用がユーザから要求される毎に、要求されている機能の利用権限をユーザが有しているか否かを判断するので、上記効果に加え、各アプリケーション・システムが提供可能な個々の機能が、利用権限のないユーザによって不正に利用されることを確実に阻止することができる、という効果を有する。

【0114】請求項6記載の発明は、請求項1記載の発明において、正当な利用者であることを確認できたユーザに対してチケット情報を与え、各アプリケーション・システムは、提供可能な機能の利用を要求しているユーザが正当なチケット情報を所持しているか否かを判断することで、前記ユーザが正当な利用者か否かを判定する

特開2003-67336

28

ので、上記効果に加え、確認・許可手段による正当な利用者であることの確認を経ることなく、コンピュータ・システムが不正利用されることを阻止することができる、という効果を有する。

【0115】請求項8記載の発明は、請求項6記載の発明において、確認・許可手段に異常が生じた場合に、コンピュータ・システムへのユーザのログイン要求に対し、障害用チケット情報をユーザに与えるようにしたので、上記効果に加え、確認・許可手段に異常が生じた場合にも、正当な利用者が全てのアプリケーション・システムを利用できない状態に陥ることを回避できる、という効果を有する。

【図面の簡単な説明】

【図1】 本実施形態に係るコンピュータ・システムの概略構成を示すブロック図である。

【図2】 RTGSシステムのユーザ情報設定画面の一例を示すイメージ図である。

【図3】 RAPIDシステムのユーザ情報設定画面の一例を示すイメージ図である。

【図4】 RAPIDシステムのユーザ情報設定画面の一例を示すイメージ図である。

【図5】 クライアントPCで実行されるMIシステム利用処理の内容を示すフローチャートである。

【図6】 運用管理サーバで実行されるMI運用管理処理の内容を示すフローチャートである。

【図7】 アプリケーション・サーバで実行されるMIアプリケーション処理の内容を示すフローチャートである。

【図8】 MIログイン画面の一例を示すイメージ図である。

【図9】 MIメニュー画面の一例を示すイメージ図である。

【図10】 RTGSシステムのメニューバーの一例を示すイメージ図である。

【図11】 RAPIDシステムのメインメニュー画面の一例を示すイメージ図である。

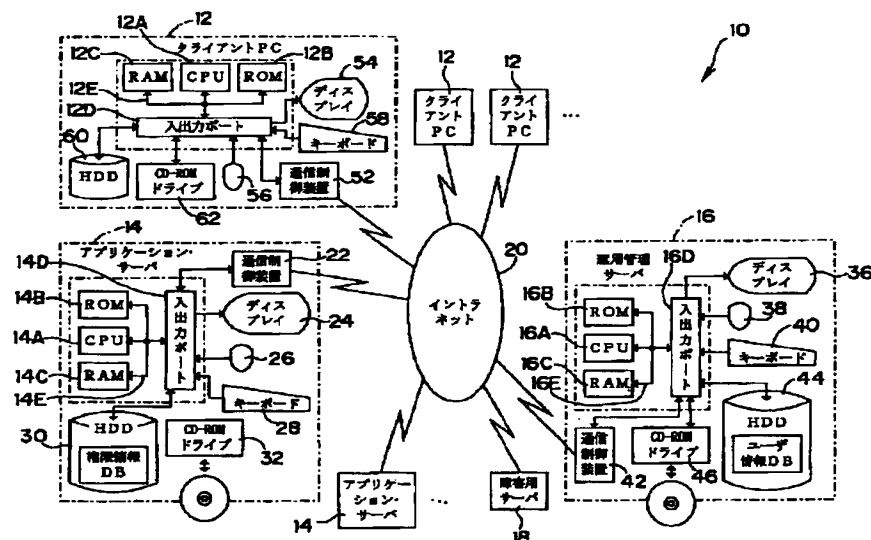
【符号の説明】

- 10 コンピュータ・システム
- 12 クライアントPC
- 14 アプリケーション・サーバ
- 16 運用管理サーバ
- 18 障害用サーバ
- 20 イン트라ネット
- 30 HDD
- 44 HDD
- 54 ディスプレイ
- 56 マウス
- 58 キーボード

(16)

特開2003-67336

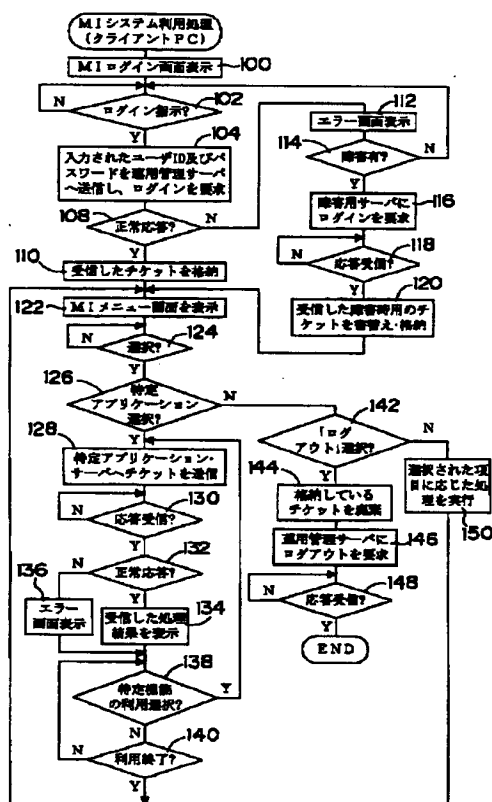
【図1】



【図2】

【図8】

【図5】



(17)

特開2003-67336

【図3】

MSN210400

新門賃金システム (RAPID) オペレーション/機能登録 2000/08/22 資金正数帳

機能区分 ☒ 新規 ☐ 変更
機能カテゴリ ☒ 運用基本/バネース管理 ☐ 業務基本

機能バネース番号 (1~50までの入力が可能です)

機能バネース番号 使用ユーザ数 機能バネースメニュー数

| | | |
|----|----|----|
| 1 | 2 | 10 |
| 2 | 1 | 10 |
| 3 | 0 | 3 |
| 6 | 11 | 3 |
| 20 | 0 | 0 |
| 30 | 0 | 0 |
| 40 | 0 | 0 |
| 50 | 0 | 0 |

メニューボタン名

| | |
|-----------|----------------|
| MSN100100 | フロント画面運用メニュー設定 |
| MSN100200 | タイマアラーム設定 |
| MSN210100 | ユーザ情報一覧画面 |
| MSN210200 | ユーザ情報編集画面 |
| MSN210300 | オペレーション情報検索画面 |
| MSN210400 | オペレーション情報管理画面 |
| MSN220100 | 取引先一覧画面 |
| MSN220200 | 取引先詳細画面 |
| MSN220300 | フロント取引先登録一覧 |
| MSN220500 | 取引先停止一覧 |

戻る(F4) 確認(F11) 実行(F2)

(※画面) 70000に接続しました。

【図4】

MSN210200

新門賃金システム (RAPID) ユーザ情報登録 2000/08/17 資金正数帳

変更区分 ☐ 新規 ☒ 変更
ユーザID

有線区分 ☒ 有線 ☐ 無線
氏名

行員番号

所属部署

役職

担当コード

組織コード

オペレーション/機能区分

機能バネース(運用/バネース)

機能バネース(機能)

画面名称

| | |
|-----------|----------------|
| MSN100100 | フロント画面運用メニュー設定 |
| MSN100200 | タイマアラーム設定 |
| MSN210100 | ユーザ情報一覧画面 |
| MSN210200 | ユーザ情報編集画面 |
| MSN210300 | オペレーション情報検索画面 |
| MSN210400 | オペレーション情報管理画面 |
| MSN220100 | 取引先一覧画面 |
| MSN220200 | 取引先詳細画面 |
| MSN220300 | フロント取引先登録一覧 |
| MSN220500 | 取引先停止一覧 |
| MSN310100 | コールセンター |
| MSN310200 | コールセンター |
| MSN310300 | フロント画面運用メニュー設定 |
| MSN310400 | タイマアラーム設定 |
| MSN310500 | フロント画面運用メニュー設定 |
| MSN310700 | フロント画面運用メニュー設定 |
| MSN310800 | フロント画面運用メニュー設定 |
| MSN310900 | フロント画面運用メニュー設定 |
| MSN311000 | フロント画面運用メニュー設定 |
| MSN320100 | 取引先一覧画面 |
| MSN330100 | フロント画面運用メニュー設定 |
| MSN330200 | タイマアラーム設定 |
| MSN330300 | フロント画面運用メニュー設定 |
| MSN330400 | フロント画面運用メニュー設定 |
| MSN340100 | フロント画面運用メニュー設定 |
| MSN350100 | フロント画面運用メニュー設定 |
| MSN350200 | フロント画面運用メニュー設定 |

戻る(F4) 確認(F11) 実行(F2)

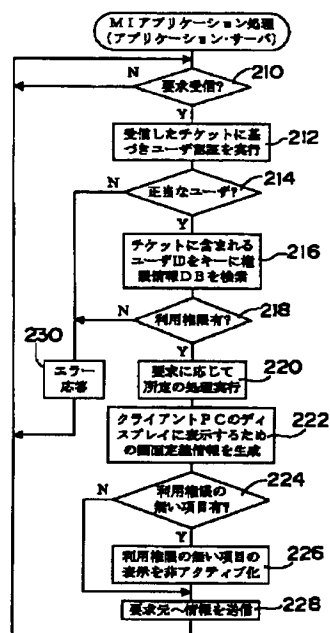
(※画面) 70000に接続しました。

【図10】

MSNシステムメニュー

ファイル(F) 当番管理(T) 設備管理(O) 決済エロル(C) 定期処理(U) マスタメンテナンス(M) 監視画面(J) オプション(O)

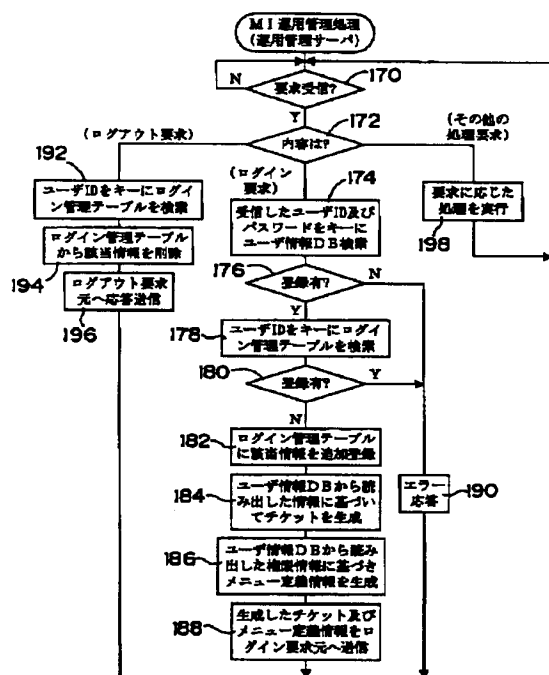
【図7】



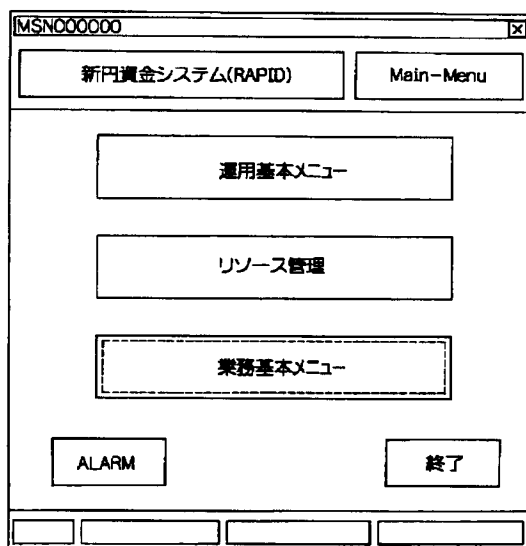
(18)

特開2003-67336

【図6】



【図11】



【図9】

